REMARKS/ARGUMENTS

Claims 1-38 are pending in the application. The Examiner has rejected claims 1-38. Applicant respectfully requests reconsideration of claims 1-38.

The Examiner has rejected claims 20-38 under 35 U.S.C. § 112 as allegedly being of undue breadth. Applicant respectfully disagrees.

Regarding claims 20-38, Applicant notes the present application, including claims 20-38, which remain in the same form in which they were originally filed, was examined and a first Office action was issued. Applicant notes that not only were claims 20-38 not determined to be of undue breadth during that examination or in that first Office action, but also specific rejections based on prior art were alleged with respect to those claims in that Office action. Accordingly, Applicant submits claims 20-38 remain in compliance with 35 U.S.C. § 112.

Moreover, while the Examiner alleges "...the claimed apparatus comprising a network element comprises a single means and therefore is regarded as undue breadth" and cites *In re Hyatt*, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983), Applicant submits the Examiner's attempt to portray claims 20-38 as "single means" claims fails to conform to MPEP § 2181, as MPEP § 2181 requires "the claim limitations must use the phrase 'means for' or 'step for'" for the claim limitation to be presumed to invoke 35 U.S.C. § 112, sixth paragraph. By contrast, Applicant notes Hyatt's claim at issue in the case the Examiner cites (i.e., Hyatt's claim 35) did use the phrase 'means for.' Thus, Applicant submits the present claims 20-38 are distinguished from Hyatt's claim 35 and MPEP § 2164.08(a) is inapplicable to claims 20-38. Accordingly, Applicant submits claims 20-38 cannot properly be considered to be of undue breadth under MPEP § 2164.08(a) and 35 U.S.C. § 112. Therefore, Applicant submits claims 20-38 are in condition for allowance.

The Examiner has rejected claims 4-16 and 23-36 under 35 U.S.C. § 112 as allegedly being indefinite to failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Applicant respectfully disagrees.

Regarding claims 4-16 and 23-36, Applicant notes the present application, including claims 4-16 and 23-36, which remain in the same form in which they were originally filed, was examined and a first Office action was issued. Applicant notes that not only were claims 4-16 and 23-36 not

determined to be indefinite during that examination or in that first Office action, but also specific rejections based on prior art were alleged with respect to those claims in that Office action. Accordingly, Applicant submits claims 4-16 and 23-36 remain in compliance with 35 U.S.C. § 112.

Moreover, Applicant submits the Examiner mischaracterizes what claims 4-16 and 23-36 actually recite in bringing the rejection. While the Examiner states, "The claim language cites a method step and apparatus functionality of "applying interface groups," Applicant notes claims 4 and 23 recite "applying interface groups to determine when marking of control packets is to be done" and claims that depend therefrom also recite subject matter beyond what the Examiner alleges. Thus, Applicant submits the actual claim language is not indefinite for failing to particularly point out and distinctly claim patentable subject matter. Therefore, Applicant submits claims 4-16 and 23-36 are in condition for allowance.

The Examiner has rejected claims 1, 2, 17, 20, 21 and 36 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McDysan et al. (U.S. Patent No. 7,046,680) in view of Ho et al. (U.S. Patent Publication No. US 2002/0116501). Applicant respectfully disagrees.

Regarding claims 1 and 20, Applicant submits the cited portions of the cited references do not render obvious the subject matter of claims 1 and 20. As an example, Applicant submits the cited portions of the cited references do not disclose or suggest "marking packets carrying the Layer-3 control information." While the Examiner cites "column 7, line 58-column 8, line 4)" of the McDysan reference as allegedly disclosing "a marker/policer 82 that marks a packet by setting bits in a DiffServ Type of Service (TOS) byte in an IP packet header," Applicant submits such teaching does not disclose "Layer-3 control information" or "marking packets carrying the Layer-3 control information." While the Examiner alleges "which is known by one of ordinary skill in the art to comprise Layer-3 control information, Applicant submits the Examiner cites no teaching in the prior art to support such assertion. Thus, Applicant submits the Examiner has not made a *prima facie* showing of obviousness with respect to claims 1 and 20.

As another example, Applicant submits the cited portions of the cited references do not disclose or suggest "encapsulating the packets at Layer-2." While the Examiner cites the Ho reference, alleging "Ho discloses encapsulating private IP packets within Layer-2 Tunneling Protocol (L2TP) messages," Applicant submits such teaching does not disclose "encapsulating the packets at Layer-2." For example, Applicant notes the current Wikipedia entry for Layer 2 Tunneling Protocol (L2TP) (copy

enclosed) states, in part, "L2TP is in fact a layer 5 protocol session layer, and uses the registered UDP port 1701." Thus, Applicant submits the Ho reference teaches away from "encapsulating the packets at Layer-2." Therefore, Applicant submits claims 1 and 20 are in condition for allowance.

Regarding claims 2 and 21, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 2 and 21. As an example, Applicant submits the cited portions of the cited references fail to disclose or suggest "marking the packets using a unique protocol identifier." While the Examiner states, "MyDysan discloses setting a DiffServ TOS byte in an IP packet header, as described with regards to Claim 1 above, therefore equivalent to Applicant's claimed functionality of marking the packets using a unique protocol identifier," Applicant submits such teaching fails to disclose or suggest "a unique protocol identifier." Also, Applicant submits the Examiner has not alleged any motivation to combine any purported teaching in the prior art as to "a unique protocol identifier." Thus, Applicant submits the Examiner has not made a *prima facie* showing of obviousness with respect to claims 2 and 21. Therefore, Applicant submits claims 2 and 21 are in condition for allowance.

Regarding claims 17 and 36, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 17 and 36. As an example, Applicant submits the cited portions of the cited references fail to disclose or suggest "encapsulating the packets according to control encapsulation." While the Examiner cites "(paragraph 0055)" of the Ho reference, Applicant submits the cited portion of the cited reference teaches away from the subject matter of claims 17 and 36. Applicant notes "(paragraph 0055)" of the Ho reference states, in part, "Control messages 48 are sent over L2TP control channel 44 that transmits packets in-band over the same packet transport layer 4. The packet transport layer 4 overlays the IP network 3. Thus, the information in the packet transport layer 4 is in turn sent over the internet protocol layer 3." Applicant submits such teaching teaches away from "encapsulating the packets at Layer-2." Therefore, Applicant submits claims 17 and 36 are in condition for allowance.

Regarding claims 3 and 22, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 3 and 22. As an example, Applicant submits the cited portions of the cited references fail to disclose or suggest "marking the packets using a link-local MPLS label." While the Examiner cites "(paragraphs 0065 and 0066)" of the Nakamichi reference, Applicant notes "(paragraphs 0065 and 0066)" of the Nakamichi refer to "the opaque LSA." Applicant further notes paragraph [0050] of the Nakamichi reference states, "...an opaque LSA (Link State

Advertisement) that is a peculiar LSA in OSPF (Open Shortest Path First) protocol is used." Applicant submits the Examiner does not allege motivation as to why one of ordinary skill in the art at the time the invention was made would purportedly combine of teaching as such a "peculiar LSA in OSPF" with other alleged teachings. Thus, Applicant submits the Examiner has not made a *prima facie* showing of obviousness with respect to claims 3 and 22. Therefore, Applicant submits claims 3 and 22 are in condition for allowance.

The Examiner has rejected claims 4-12 and 23-31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McDysan et al. (U.S. Patent No. 7,046,680) in view of Ho et al. (U.S. Patent Publication No. US 2002/0116501) as applied to claims 1 and 20 above, and further in view of Yu et al. (United States Patent Application Publication US 2004/0010583 A1). Applicant respectfully disagrees.

Regarding claims 4 and 23, Applicant submits the cited portions of the cited reference fail to render obvious the subject matter of claims 4 and 23. As an example, Applicant submits the cited portions of the cited references fail to disclose or suggest "applying interface groups to determine when marking of control packets is to be done." While the Examiner cites "(paragraph 0022)" and "(paragraph 0025)" of the Yu reference, Applicant submits the cited portion of the Yu reference teaches away from the subject matter of claims 4 and 23. Applicant notes "(paragraph 0022)" begins "An Interface Group is a group of interfaces selected by the network manager to collectively define when one or more network device should perform failover," which Applicant submits fails to disclose or suggest "applying interface groups to determine when marking of control packets is to be done." Applicant also notes "(paragraph 0025)" begins "The network device manager may assign a name to the interface group to enable the interface group to be referenced at a later time," which Applicant submits fails to disclose or suggest "applying interface groups to determine when marking of control packets is to be done." Therefore, Applicant submits claims 4 and 23 are in condition for allowance.

Regarding claims 5 and 24, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 5 and 24. As an example, Applicant submits the cited portions of the cited references fail to disclose or suggest "applying interface groups to packet communications within a particular interface group." While the Examiner cites "(Figure 1, interface group defined between interfaces 'a' and 'd' within network device A)" of the Yu reference, Applicant submits "Figure 1" of the Yu reference fails to disclose "interface group defined between interfaces 'a' and 'd' within network device A," as alleged by the Examiner. Thus, Applicant submits the Examiner

has not made a *prima facie* showing of obviousness with respect to the subject matter of claims 5 and 24. Therefore, Applicant submits claims 5 and 24 are in condition for allowance.

Regarding claims 6 and 25, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 6 and 25. As an example, Applicant submits the cited portions of the cited references fail to disclose or suggest "applying interface groups to packet communications within a backbone interface group." While the Examiner cites "(Figure 4, static tunnel through Internet between network device A and network device B)," Applicant submits such alleged teaching does not teach or suggest, for example, "...within a backbone interface group" or even "...interface group." Therefore, Applicant submits claims 6 and 25 are in condition for allowance.

Regarding claims 7 and 26, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 7 and 26. As an example, Applicant submits the cited portions of the cited references fail to disclose or suggest "applying interface groups to packet communications within a customer-specific interface group." While the Examiner cites "(Figure 4, interface 'a' between network device A and HostPC)," Applicant submits such alleged teaching does not teach or suggest, for example, "...within a customer-specific interface group" or even "...interface group." Therefore, Applicant submits claims 7 and 26 are in condition for allowance.

Regarding claims 8 and 27, Applicant submits the cited portions of the cited references do not render obvious the subject matter of claims 8 and 27. As an example, Applicant submits the cited portions of the cited references do not teach or suggest "applying interface groups to packet communications within a peer interface group." While the Examiner cites "(Figure 4, static tunnel between network device A and network device D)" of the Yu reference, Applicant submits such alleged teaching does not teach or suggest, for example, "...within a peer interface group" or even "...interface group." Therefore, Applicant submits claims 8 and 27 are in condition for allowance.

Regarding claims 9-12 and 28-31, Applicant submits the cited portions of the cited references do not render obvious the subject matter of claims 9-12 and 28-31. As an example, Applicant submits the cited portions of the cited references do not teach or suggest "applying interface groups to packet communications between interface groups." As another example, Applicant submits the cited portions of the cited references do not teach or suggest "applying interface groups to packet communications between backbone and customer-specific interface groups." As yet another example, Applicant submits the cited portions of the cited references do not teach or suggest "applying interface groups to

packet communications between customer-specific and peer interface groups." As a further example, Applicant submits the cited portions of the cited references do not teach or suggest "applying interface groups to packet communications between backbone and peer interface groups." Applicant notes the Examiner merely alleges teaching as to "(Figure 4, connections between peer, backbone, and customer networks at network device A)" of the Yu reference. However, Applicant submits claims 9-12 and 28-31 recite specific features, not merely "connections between peer, backbone, and customer networks." Thus, Applicant submits the Examiner has not alleged teachings as to the subject matter of claims 9-12 and 28-31. Therefore, Applicant submits the Examiner has not made a *prima facie* showing of obviousness with respect to claims 9-12 and 28-31. Moreover, Applicant note the Examiner merely alleges teaching as to "networks" not as to "interface groups." Thus, Applicant submits the Examiner has not alleged teachings as to the subject matter of claims 9-12 and 28-31. Therefore, Applicant submits the Examiner has not made a *prima facie* showing of obviousness with respect to claims 9-12 and 28-31. Accordingly, Applicant submits claims 9-12 and 28-31 are in condition for allowance.

The Examiner has rejected claims 13 and 32 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McDysan et al. (U.S. Patent No. 7,046,680) in view of Ho et al. (U.S. Patent Publication No. US 2002/0116501) and Yu et al. (United States Patent Application Publication US 2004/0010583 A1) as applied to claims 4 and 23 above, and further in view of Chuah et al. (United States Patent Application Publication US 2004/0054924 A1). Applicant respectfully disagrees.

Regarding claims 13 and 32, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 13 and 32. As an example, Applicant submits the cited portions of the cited references do not disclose or suggest "applying interface groups to communication of ICMP packets." While the Examiner cites "(paragraph 0062)" of the Chuah reference, Applicant submits "ICMP trace-backs" does not teach or suggest "applying interface groups to communication of ICMP packets." Moreover, Applicant submits the Chuah reference teaches away from the subject matter of claims 13 and 32, as Applicant notes "(paragraph 0062)" of the Chuah reference refers, in the alternative, to "probabilistic marking of IP packets" and "intentional ICMP trace-backs." Therefore, Applicant submits claims 13 and 32 are in condition for allowance.

The Examiner has rejected claims 14 and 33 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McDysan et al. (U.S. Patent No. 7,046,680) in view of Ho et al. (U.S. Patent Publication No. US 2002/0116501) and Yu et al. (United States Patent Application Publication US

2004/0010583 A1) as applied to claims 4 and 23 above, and further in view of Pan et al. (United States Patent 7,336,615). Applicant respectfully disagrees.

Regarding claims 14 and 33, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 14 and 33. As an example, Applicant submits the cited portions of the cited references do not disclose or suggest "applying interface groups to communication of ping packets." While the Examiner cites "(column 14, lines 48-55)" of the Pan reference, Applicant submits the Examiner's characterization that "Pan discloses assigning predetermined port numbers to LSP ping messages" teaches away from what the Examiner alleges teaches "interface groups" in claims from which claims 14 and 33 depend. Thus, Applicant submits the Examiner's alleged combination would be rendered inoperable. Therefore, Applicant submits claims 14 and 33 are in condition for allowance.

The Examiner has rejected claims 15 and 34 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McDysan et al. (U.S. Patent No. 7,046,680) in view of Ho et al. (U.S. Patent Publication No. US 2002/0116501) and Yu et al. (United States Patent Application Publication US 2004/0010583 A1) as applied to claims 4 and 23 above, and further in view of Fotedar et al. (United States Patent Application Publication 2004/0085965 A1). Applicant respectfully disagrees.

Regarding claims 15 and 34, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 15 and 34. As an example, Applicant submits the cited portions of the cited references do not disclose or suggest "applying interface groups to communication of traceroute packets." While the Examiner cites "(paragraph 0011)" of the Fotedar reference, Applicant submits the Examiner's characterization that "Fotedar discloses assignment of traceroute packets to a virtual router address indicative of a loopback interface" teaches away from what the Examiner alleges teaches "interface groups" in claims from which claims 15 and 34 depend. Thus, Applicant submits the Examiner's alleged combination would be rendered inoperable. Therefore, Applicant submits claims 15 and 34 are in condition for allowance.

The Examiner has rejected claims 18 and 37 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McDysan et al. (U.S. Patent No. 7,046,680) in view of Ho et al. (U.S. Patent Publication No. US 2002/0116501) as applied to claims 1 and 20 above, and further in view of Johansson (United States Patent 6,061,330). Applicant respectfully disagrees.

Regarding claims 18 and 37, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 18 and 37. As an example, Applicant submits the cited portions of the cited references do not disclose or suggest "receiving unmarked control packets using rate-limited queues." Applicant notes the Examiner cites "(Figure 1, 116; Figure 4, 410)" of the Johansson reference. Applicant sees no "Figure 4" in the Johansson reference, so Applicant assumes the Examiner is referring to "Figure 4a, 410." Applicant submits the Examiner mischaracterizes the teachings of the Johansson reference. As an example, Applicant notes the Johansson reference states, in col. 9, lines 41-43, "The flow diagram of FIG. 4a illustrates steps for calculating aggregated offered rate y_{tot} and queue length at the output device 224." Applicant submits "the output device 224" teaches away from "receiving unmarked control packets using rate-limited queues." Moreover, Applicant submits the Examiner has not alleged any relationship between "the output device 224" and "Figure 1, 116." Thus, Applicant submits the Examiner has not made a *prima facie* showing of obviousness with respect to claims 18 and 37. Therefore, Applicant submits claims 18 and 37 are in condition for allowance.

The Examiner has rejected claims 19 and 38 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McDysan et al. (U.S. Patent No. 7,046,680) in view of Ho et al. (U.S. Patent Publication No. US 2002/0116501) as applied to claims 1 and 20 above, and further in view of Hussey et al. (United States Patent Application Publication 2001/0049744 A1). Applicant respectfully disagrees.

Regarding claims 19 and 38, Applicant submits the cited portions of the cited references fail to render obvious the subject matter of claims 19 and 38. As an example, Applicant submits the cited portions of the cited references do not disclose or suggest "processing the received packets at a line rate." While the Examiner cites "(paragraph 0050)" of the Hussey reference, Applicant notes "(paragraph 0050)" of the Hussey reference does not specifically recite "a processor pool aggregation technique wherein a received packet data stream is capable of being processed at a line rate," but instead states "...receives a packet data stream via the communication network 110 at a line rate that might otherwise overwhelm the processing capabilities of the NIC 160 and result in dropped packets and reduced quality of service." Moreover, Applicant submits the Examiner has not presented any evidence that the purported combination of the teachings of Hussey and those of the other cited references would not also "otherwise overwhelm the processing capabilities of the NIC 160 and result in dropped packets and reduced quality of service." Accordingly, Applicant submits the Examiner's
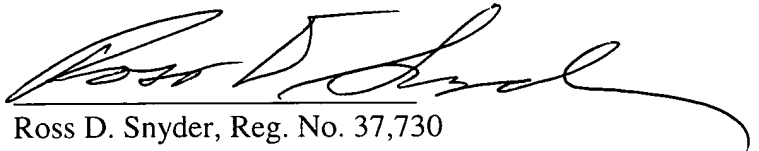
purported combination has not been shown to disclose or suggest the subject matter of claims 19 and 38. Therefore, Applicant submits claims 19 and 38 are in condition for allowance.

In conclusion, Applicant has overcome all of the Office's rejections, and early notice of allowance to this effect is earnestly solicited. If, for any reason, the Office is unable to allow the Application on the next Office Action, and believes a telephone interview would be helpful, the Examiner is respectfully requested to contact the undersigned attorney.

Respectfully submitted,

07/23/2008
Date

Ross D. Snyder, Reg. No. 37,730
Attorney for Applicant(s)
Ross D. Snyder & Associates, Inc.
PO Box 164075
Austin, Texas 78716-4075
(512) 347-9223 (phone)
(512) 347-9224 (fax)

Layer 2 Tunneling Protocol

From Wikipedia, the free encyclopedia

In computer networking, the **Layer 2 Tunneling Protocol (L2TP)** is a tunneling protocol used to support virtual private networks (VPNs).

Contents

History and future

Published in 1999 as proposed standard RFC 2661, L2TP has its origins primarily in two older tunneling protocols for PPP: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). A new version of this protocol, L2TPv3, was published as proposed standard RFC 3931 in 2005. L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network (e.g., Frame Relay, Ethernet, ATM, etc).

Description

L2TP acts like a data link layer (layer 2 of the OSI model) protocol for tunneling network traffic between two peers over an existing network (usually the Internet). L2TP is in fact a layer 5 protocol session layer, and uses the registered UDP port 1701. The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. It is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel while the LNS is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this an L2TP session (or *call*) is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP.

The packets exchanged within an L2TP tunnel are categorised as either control packets or data packets. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel.

Tunneling Models

An L2TP tunnel can extend across an entire PPP session or only across one segment of a two-segment session. This can be represented by four different tunneling models, namely [1] [2] [3]

1. *voluntary tunnel*
2. *compulsory tunnel — incoming call*

3. *compulsory tunnel — remote dial* and
4. *L2TP multi-hop connection*

In the voluntary tunnel model, a tunnel is created by the user, typically by the use of an L2TP enabled client which is called the LAC client. The user will send L2TP packets to the Internet Service Provider (ISP) which will forward them on to the LNS. The ISP does not need to support L2TP, it only forwards the L2TP packets between LAC and LNS. The LAC client acts as an L2TP tunnel initiator which effectively resides on the same system as the remote client. The tunnel extends across the entire PPP session from the L2TP client to the LNS.

In the compulsory tunnel model-incoming call, a tunnel is created between ISP LAC and the LNS home gateway. The company may provide the remote user with a Virtual Private Network (VPN) login account from which he can access the corporate server. As a result the user will send PPP packets to the ISP (LAC) which will encapsulate them in L2TP and tunnel them to the LNS. In the compulsory tunneling cases, the ISP must be L2TP capable. In this model the tunnel only extends across the segment of the PPP session between the ISP and the LNS.

In the compulsory tunnel model-remote dial the home gateway (LNS) initiates a tunnel to an ISP (LAC) (outgoing call) and instructs the ISP to place a local call to the PPP enabled client which is the remote user. This model is intended for cases where the remote PPP Answer Client has a permanently established phone number with an ISP. This model is expected to be used when a company with established presence on the Internet needs to establish a connection to a remote office that requires a dial-up link. In this model the tunnel only extends across the segment of the PPP session between the LNS and the ISP.

An L2TP Multi-hop connection is a way of redirecting L2TP traffic on behalf of client LACs and LNSs. A Multi-hop connection is established using an L2TP Multi-hop gateway. A tunnel is established from a client LAC to the L2TP Multi-hop gateway and then another tunnel is established between the L2TP Multi-hop gateway and a target LNS. L2TP traffic between client LAC and LNS is redirected to each other through the gateway.

L2TP Packet Structure

An L2TP packet consists of :

0 - 15 bit	16 - 31 bit
Flags and Version Info	Length (opt)
Tunnel ID	Session ID
Ns (opt)	Nr (Opt)
Offset Size (opt)	Offset Pad (Opt)......
Payload data	

Field meanings:

Flags and version
    control flags indicating Data/Control packet and presence of length, sequence, offset fields.
Length (optional)
    Total length of the message in bytes, present only when length flag is set.
Tunnel ID
    Indicates the identifier for the control connection.
Session ID
    Indicates the identifier for a session within a tunnel.
Ns (optional)
    sequence number for this data or control message, beginning at zero and incrementing by one (modulo 2**16) for each message sent. Present only when sequence flag set.
Nr (optional)
    sequence number for expected message to be received. Nr is set to the Ns of the last in-order message received plus one (modulo 2**16). In data messages, Nr is reserved and, if present (as indicated by the S bit), MUST be ignored upon receipt..
Offset Size (optional)
    Specifies where payload data is located past the L2TP header Actual data within the offset padding is undefined. If the offset field is present, the L2TP header ends after the last byte of the offset padding. This field exists if the offset flag is set.

Offset Pad (optional)
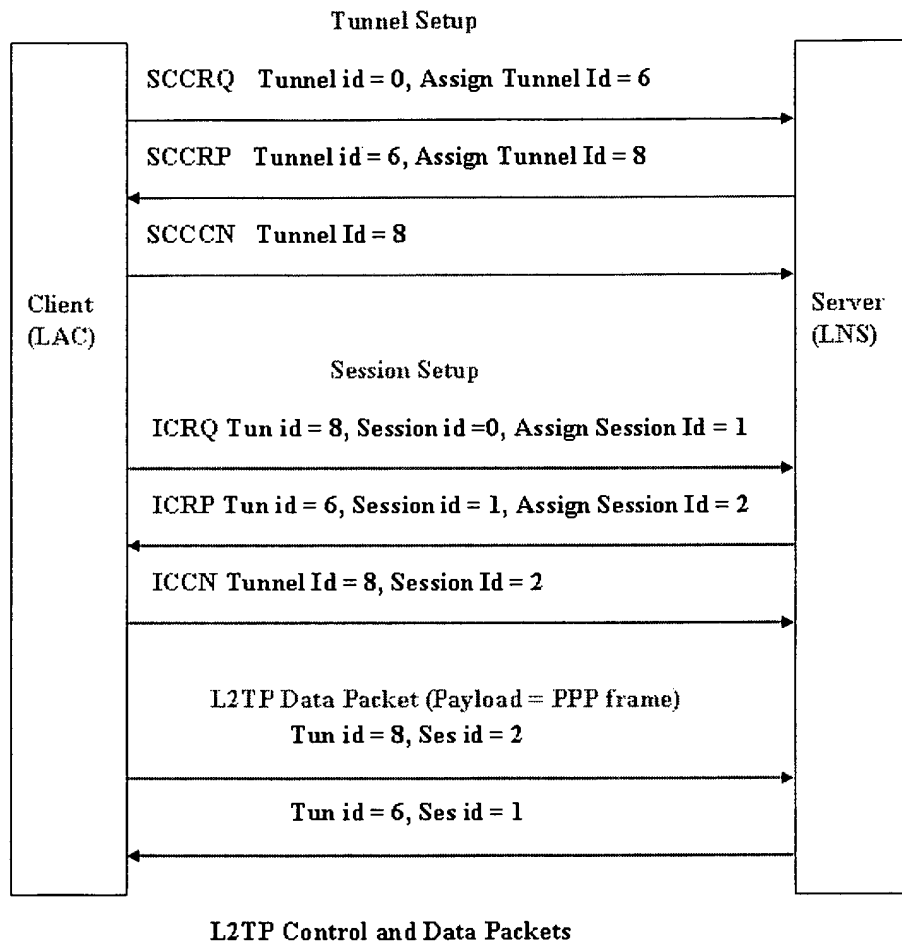>   Variable length
Payload data
>   Variable length (Max payload size = Max size of UDP packet - size of L2TP header)

L2TP Packet Exchange

At the time of setup of L2TP connection, many control packets are exchanged between server and client to establish tunnel and session for each direction. One peer requests other peer to assign a specific tunnel and session id through these control packets. Then using this tunnel and session id data packets are exchanged with the compressed PPP frames as payload.

The list of L2TP Control messages exchanged between LAC and LNS, for handshaking before establishing a tunnel and session in voluntary tunneling method are

Tunnel Setup

SCCRQ Tunnel id = 0, Assign Tunnel Id = 6	→
SCCRP Tunnel id = 6, Assign Tunnel Id = 8	←
SCCCN Tunnel Id = 8	→

Client (LAC) ... Server (LNS)

Session Setup

ICRQ Tun id = 8, Session id =0, Assign Session Id = 1	→
ICRP Tun id = 6, Session id = 1, Assign Session Id = 2	←
ICCN Tunnel Id = 8, Session Id = 2	→
L2TP Data Packet (Payload = PPP frame) Tun id = 8, Ses id = 2	→
Tun id = 6, Ses id = 1	←

L2TP Control and Data Packets

L2TP/IPsec

Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. This is referred to as L2TP/IPsec, and is standardized in IETF RFC 3193. The process of setting up an L2TP/IPsec VPN is as follows:

1. Negotiation of IPsec Security Association (SA), typically through Internet Key Exchange (IKE). This is carried out over UDP port 500, and commonly uses either a shared password (so-called "pre-shared keys"), public keys, or X.509 certificates on both ends, although other keying methods exist.
2. Establishment of Encapsulating Security Payload (ESP) communication in transport mode. The IP Protocol number for ESP is 50 (compare TCP's 6 and UDP's 17). At this point, a secure channel has been established, but no tunneling is taking place.

3. Negotiation and establishment of L2TP tunnel between the SA endpoints. The actual negotiation of parameters takes place over the SA's secure channel, within the IPsec encryption. L2TP uses UDP port 1701.

When the process is complete, L2TP packets between the endpoints are encapsulated by IPsec. Since the L2TP packet itself is wrapped and hidden within the IPsec packet, no information about the internal private network can be garnered from the encrypted packet. Also, it is not necessary to open UDP port 1701 on firewalls between the endpoints, since the inner packets are not acted upon until after IPsec data has been decrypted and stripped, which only takes place at the endpoints.

A potential point of confusion in L2TP/IPsec is the use of the terms "tunnel" and "secure channel." *Tunnel* refers to a channel which allows untouched packets of one network to be transported over another network. In the case of L2TP/IPsec, it allows L2TP/PPP packets to be transported over IP. A *secure channel* refers to a connection within which the confidentiality of all data is guaranteed. In L2TP/IPsec, first IPsec provides a secure channel, then L2TP provides a tunnel.

Windows Implementation

Windows versions before Vista were very difficult to configure for IPsec without L2TP. Microsoft boasts that they have reduced the complexity: they say that in Windows 2000/XP it required more than 100 mouseclicks to set up an IPsec VPN connection, and in Vista it requires "only" 15 mouseclicks. There is also slightly more help info in Vista compared to XP, such as "What is a VPN?" but this is generally very basic info. The help info does say that IPsec without L2TP is not to be used for Road Warrior-style VPNs. They advise to use L2TP/IPsec or PPTP for that.

There are two new configuration utilities in Windows Vista that attempt to make IPsec without L2TP easier:

- an MMC snap-in called "Windows Firewall with Advanced Security" (WFwAS), located in Control Panel -> Administrative Tools. Discussed in the section below.
- the "netsh advfirewall" command-line tool. Discussed in another section below.

Unfortunately, both these configuration utilities experience a couple of problems.

The first problem is that there is almost no documentation about both "netsh advfirewall" and the IPsec client in WFwAS. Problem #2 is that there is a bug in Vista: when certificate-based authentication is involved Vista currently cannot process packets that it receives from the Openswan server. This problem is reported to be fixed in Vista SP1. The third problem is that things don't work at all if NAT is involved. A fourth problem is that you can only specify server IP addresses in the new Vista configuration utilities. You cannot specify the hostname of the server, so if the IP address of the IPsec server changes, all clients will have to be informed of this new IP address (this also rules out servers that addressed by DynDNS or something similar).

L2TP in ADSL networks

L2TP is often used as a tunneling mechanism to resell ADSL endpoint connectivity. An L2TP tunnel would sit between the user and the ISP the connection would be resold to, so the reselling ISP would not appear as doing the transport.

L2TP in CABLE networks

L2TP is used by the Cable providers (HOT in Israel for example) as a tunneling mechanism to sell endpoint connectivity. This L2TP tunnel sits between the user and the ISP the connection has been sold by; And again the reselling cable provider doesn't appear as doing the transport.

External links

Implementations

- 6WIND, 6WINDGate L2TP for SoC and multi-core network processors
- Cisco: Cisco L2TP documentation, also read Technology brief from Cisco
- Open source and Linux: xl2tpd, Linux RP-L2TP, OpenL2TP, l2tpns, l2tpd (inactive), Linux L2TP/IPsec server, FreeBSD multi-link PPP daemon
- Microsoft: built-in client included with Windows 2000 and higher; Microsoft L2TP/IPsec VPN Client for Windows 95/98/NT
- Apple: built-in client included with Mac OS X 10.3 and higher.

Internet standards and extensions

- RFC 2341 Cisco Layer Two Forwarding (Protocol) "L2F". *(A predecessor to L2TP)*
- RFC 2637 Point-to-Point Tunneling Protocol (PPTP). *(A predecessor to L2TP)*
- RFC 2661 **Layer Two Tunneling Protocol "L2TP"**
- RFC 2809 Implementation of L2TP Compulsory Tunneling via RADIUS
- RFC 2888 Secure Remote Access with L2TP
- RFC 3070 Layer Two Tunneling Protocol (L2TP) over Frame Relay
- RFC 3145 L2TP Disconnect Cause Information
- RFC 3193 Securing L2TP using IPsec
- RFC 3301 Layer Two Tunnelling Protocol (L2TP): ATM access network
- RFC 3308 Layer Two Tunneling Protocol (L2TP) Differentiated Services
- RFC 3355 Layer Two Tunnelling Protocol (L2TP) Over ATM Adaptation Layer 5 (AAL5)
- RFC 3371 Layer Two Tunneling Protocol "L2TP" Management Information Base
- RFC 3437 Layer Two Tunneling Protocol Extensions for PPP Link Control Protocol Negotiation
- RFC 3438 Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update
- RFC 3573 Signaling of Modem-On-Hold status in Layer 2 Tunneling Protocol (L2TP)
- RFC 3817 Layer 2 Tunneling Protocol (L2TP) Active Discovery Relay for PPP over Ethernet (PPPoE)
- RFC 3931 Layer Two Tunneling Protocol - Version 3 (L2TPv3).
- RFC 4045 Extensions to Support Efficient Carrying of Multicast Traffic in Layer-2 Tunneling Protocol (L2TP).
- RFC 4951 Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover".

Other

- IANA assigned numbers for L2TP
- L2TP Extensions Working Group (l2tpext) - *(where future standardization work is being coordinated)*
- Using Linux as an L2TP/IPsec VPN client

Retrieved from "http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol"
Categories: VPN | Internet protocols | Internet standards | Tunneling protocols